(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 197 33 662 C 1**

(51) Int. Cl.[6]:
H 04 Q 7/34
H 04 M 1/66
H 04 B 1/38
H 04 Q 7/38

(21) Aktenzeichen: 197 33 662.0-31
(22) Anmeldetag: 4. 8. 97
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 7. 1. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
DeTeMobil Deutsche Telekom MobilNet GmbH, 53227 Bonn, DE

(72) Erfinder:
Dupré, Michael, 53757 Sankt Augustin, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 1 95 27 715 A1

(54) Verfahren und Vorrichtung zur kundenseitigen Personalisierung von GSM-Chips

(57) Es wird ein Verfahren zur Personalisierung von GSM-Chips beschrieben, in deren Speicherbereich mindestens eine Teilnehmer-Kennung IMSI und eine Kartennummer ICCID eingespeichert ist, und wobei zwecks Personalisierung dem Chip noch ein geheimer Schlüssel Ki und ggf. weitere Daten eingespeichert sind. Es soll ein unnötig großer Verwaltungsaufwand zur Verwaltung aller Kartendaten im Authentifikationszentrum AC entfallen und die Aufbewahrung der geheimen Daten des Chips soll sicherer ausgebildet werden. Die Erfindung sieht vor, daß der Chip die endgültigen Daten erst dann eingeschrieben erhält, wenn der Teilnehmer sich in das Teilnehmernetz einbucht. Damit besteht der Vorteil, daß in die Karte lediglich anfängliche Daten eingeschrieben werden, mit denen der Kunde lediglich in der Lage ist, erstmalig mit dem Rechenzentrum des Netzbetreibers Kontakt aufzunehmen. Bei diesem erstmaligen Kontakt werden dann die endgültigen Daten zwischen der Karte und dem Rechenzentrum ausgehandelt und in die Karte eingeschrieben. Das Rechenzentrum braucht deshalb nur die Karten zu verwalten, die auch tatsächlich an Kunden vergeben wurden.

DE 197 33 662 C 1

DE 197 33 662 C 1

Beschreibung

Vorgeschlagen wird ein Verfahren zur kundenseitigen Personalisierung von GSM-Chips, bei dem davon ausgegangen wird, daß sich der Chip zum Zeitpunkt der Personalisierung im Endgerät des Kunden befindet.

Nach dem Stand der Technik ist der GSM-Chip bei den Netzbetreibern zur Zeit in einer GSM-Karte implementiert, die in das Endgerät eingesteckt wird. Dieser Chip könnte genausogut fest in das Endgerät integriert sein., z. B. auf einer Einschubkarte eines Computers. Bei dem vorliegenden Verfahren spielt es also keine Rolle, ob eine GSM-Karte oder ein Endgerät mit integriertem Chip verwendet wird. Unter dem Begriff "Chip" wird im weitesten Sinne ein EPROM, ein EEPROM oder auch ein "intelligenter" Mikroprozessor verstanden.

Ohne Beschränkung auf eine bestimmte Ausführungsform ist im folgenden von einem "Chip" und dem "Chiphersteller" die Rede.

Bei der bisherigen, zentralen Personalisierung erhält der Chip neben anderen Daten eine Kartennummer (ICCID), eine Teilnehmerkennung (IMSI) und mehrere Geheimzahlen eingeschrieben. Während der Chiphersteller ohne weiteres die Daten ICCID und IMSI in den Chip einbringen könnte, möchte der Netzbetreiber gerne selbst die Kontrolle über die Geheimzahlen, insbesondere über den Schlüssel Ki, der nur der Karte und dem Netz bekannt sein soll, behalten.

Bei der gegenwärtigen, zentralen Personalisierung bekommt der Netzbetreiber Rohkarten vom Kartenhersteller und schreibt dann den endgültigen, geheimen Schlüssel hinein. Dieser Schlüssel ist dann nur zwei Stellen bekannt, nämlich dem Chip selbst und dem Netzbetreiber.

Nachteilig hierbei ist, daß im Rechenzentrum des Netzbetreibers eine außerordentlich hohe statische Last erzeugt wird. Mit einem Generator werden eine Vielzahl von Schlüsseln erzeugt, die dann in die jeweiligen Karten eingebracht werden. Man schickt dann gleichzeitig den jeweils pro Karte erzeugten Schlüssel zum Rechenzentrum (Authentifikationszentrum AC), und danach wird die Karte an die Verkaufsorganisationen herausgegeben. Das AC hat also im Moment der Herausgabe der jeweiligen Karte bereits alle Teilnehmerkennungen IMSI und die dazugehörenden geheimen Schlüssel Ki gespeichert und muß diese verwalten, obwohl die jeweilige Karte noch irgendwo beim Händler liegt und noch gar nicht verkauft worden ist. Bei über 17.000 Verkaufsstellen liegen also Karten, die noch nicht verkauft wurden und deren Daten aber trotzdem vom AC verwaltet werden müssen.

Außerdem besteht prinzipiell die Gefahr, daß wenn ein Hersteller oder irgendein anderes Mitglied der Verkaufsorganisation die Karten personalisieren soll, es sein könnte, daß dieser Schlüssel kompromittiert ist. Die anfängliche Personalisierung des Chip ist also unsicher und mit der Gefahr des Mißbrauchs behaftet.

Die DE 195 27 715 A1 betrifft ein Verfahren zur Nutzer-Identifikation und -authentifikation bei Datenfunkverbindungen, wobei hier zur Authentifikation von Teilnehmern sogenannte Chipkarten eingesetzt werden, in deren Speicherbereich teilnehmerspezifische Daten abgelegt sind. Die Identität des Teilnehmers wird also, wie bei GSM üblich, über eine personenbezogene Chipkarte überprüft, wobei die Personalisierung der Chipkarte beim Netzbetreiber selbst vor der Übermittlung an den Teilnehmern erfolgt.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren, eine Vorrichtung und einen Chip der eingangs genannten Art so weiterzubilden, daß ein unnötig großer Verwaltungsaufwand im AC entfallen kann und daß die Aufbewahrung der geheimen Daten des Chip sicherer ausgebildet ist.

Zur Lösung der gestellten Aufgabe ist die Erfindung durch die technische Lehre des Anspruchs 1 gekennzeichnet. Ein Chip nach der Erfindung ist durch die technische Lehre der Ansprüche 6 bis 10 gekennzeichnet. Im übrigen wird die Vorrichtung zur kundenseitigen Personalisierung des GSM-Chips in den Ansprüchen 11 bis 13 beschrieben.

Mit der erfindungsgemäßen technischen Lehre werden insbesondere folgende Vorteile erreicht:

- Vermeidung einer zentralen Personalisierung beim Netzbetreiber
- Ausgabe von sehr vielen GSM-Chips ohne Erzeugung einer statischen Last beim Netzbetreiber
- Wiederverwendung von "gebrauchten" GSM-Chips
- Regelmäßiger Wechsel des secret Key Ki während der Nutzungsdauer durch den Kunden.

Mit dem hier vorgestellten Verfahren bringt der Gerätehersteller/Chiphersteller initiale kartenbezogene Daten in den Chip ein, sozusagen eine Vorpersonalisierung. Die eigentliche Personalisierung nimmt der Netzbetreiber selbst zu einem späteren Zeitpunkt vor, und auch nur bei den Kunden, die ein Vertragsverhältnis mit dem Netzbetreiber eingehen.

Die Vorpersonalisierung erzeugt bei dem Netzbetreiber noch keine statische Last. Das Verfahren bietet somit die Voraussetzung, um "Millionen" von GSM-Chips zu verteilen, z. B. in jedes Auto, in jeden Laptop oder in jede Alarmanlage, und später nur die Chips der Kunden zu "aktivieren", die ein Vertragsverhältnisse eingehen.

Des weiteren ist es möglich, Karten wiederzuverwenden, falls ein Kunde sein Vertragsverhältnis kündigt (z. B. bei Verkauf seines Autos).

Speziell beim Netzbetreiber D1 könnte der Händler zurückgegebene Karten erneut für einen anderen Kunden freischalten. Der Netzbetreiber spart somit die Personalisierung von Karten für das Austauschgeschäft ein.

Zur Verwirklichung der technischen Lehre wird es bevorzugt, wenn der GSM-Chip Toolkit fähig ist. Insbesondere sollte das Endgerät Short Messages zum Netzbetreiber schicken können.

Außerdem sollte der Chip eine Funktion anbieten, den Chip wieder initial zu machen (s. u.).

Im übrigen kann auch das Endgerät oder ein anderes Gerät diese Funktion des Chip nutzen.

Die Kartennummer und die Versionsnummer (s. u.) sollten durch das Endgerät auslesbar sein (oder auf der GSM-Karte sichtbar sein).

Der Chiphersteller ist für die Vorpersonalisierung zuständig.

ICCID und IMSI werden einem Nummernpool entnommen, der Chip selbst leitet sich aus einem Schlüssel K1, den der Chiphersteller kennt, einen initialen Ki_1 ab. PIN und PUK werden auf einen Defaultwert gesetzt.

- Im AC erfolgt kein Eintrag
- Wird ein Kunde gewonnen, erfolgt ein Eintrag im AC. Dieses leitet sich ebenfalls den initialen Key Ki_1 ab.
- Im HLR wird das Hotlining Flag gesetzt
- Der erste Call wird zu einem Security Center geroutet
- Dieses handelt mit dem Verfahren nach Diffie-Hellman einen neuen Ki_2 sowie einen PUK aus.
- Gebrauchte Chips, die wiederverwendet werden sollen, werden mit einer internen Funktion zurückgesetzt.

Die Vorpersonalisierung beim Chiphersteller erfolgt dergestalt, daß jeder Chiphersteller einen Bereich von Kartennummern und Teilnehmerkennungen zugeteilt bekommt. Die Nummernbereiche für ICCID und IMSI sind so groß, daß dies möglich ist.

Weiterhin erhält der Chiphersteller folgende Daten vom Netzbetreiber: a, p, VER, K1.

Der Chiphersteller bringt dann folgende Daten in jeden Chip ein:

- ICCID Kartennummer
- IMSI Teilnehmerkennung
(ist an ICCID gebunden, z. B. gleiche Position innerhalb der beiden Nummernbereiche für ICCID und IMSI)
- a hinreichend große Zahl, Basis für Diffie-Hellman.
- p hinreichend große Zahl, Primzahl für Diffie-Hellman
- VER Versionsnummer, z. B. 8 Byte, eindeutig je Chiphersteller (kann öfters gewechselt werden)
- K1 8 Byte DES-Schlüssel, eindeutig an VER gebunden

Bemerkung: Der Netzbetreiber könnte sich mit einem Masterkey den Schlüssel K1 aus der Versionsnummer VER ableiten (z. B. mit DES-Verfahren). Dies ist aber nicht notwendig.

Der Chip generiert sich dann folgende Geheimzahlen:

- Ki_1 Ki_1 ist ein initialer Ki, den der Chip mit dem DES-Schlüssel K1 aus der IMSI ableitet.
- PIN Die PIN wird fest auf 0000 gesetzt
- PUK Der PUK wird fest auf 00000000 gesetzt
- ggf. weitere Geheimzahlen.

Der Chip muß K1 und die generierten Geheimzahlen in einem sicheren Bereich halten und vor Auslesen schützen.

Die Vorgänge im Authentifikationszentrum AC

- Das AC kennt von jeder Versionsnummer VER den Schlüssel K1 (kann K1 mit einem Masterkey aus VER abgeleitet werden, brauchen die an die Chiphersteller ausgegebenen K1 nicht gespeichert zu werden)
- Die von den Chips generierten initialen Ki_1 werden nicht in das AC eingetragen
Das AC kennt auch die IMSIs noch nicht, somit ist keine statische Last vorhanden

Kundengewinnung und Freischaltung durch den Netzbetreiber

Möchte ein Kunde sein Gerät (seine Karte, seinen Chip) nutzen, geht er mit dem Netzbetreiber einen Vertrag ein. Die Kartennummer (ICCID) identifiziert den Chip.

Der Netzbetreiber veranlaßt folgende Aktionen:

- Auslesen oder Ablesen von Kartennummer und Versionsnummer (ICCID, VER)
- Der ICCID ist die IMSI fest zugeordnet
- im AC werden IMSI und VER eingetragen (jetzt erst wird das Teilnehmerverhältnis im AC bekannt gemacht)
- Das AC kennt den Schlüssel K1, der fest an VER gebunden ist und generiert sich aus K1 den initialen Schlüssel
Ki_1 nach dem gleichen Verfahren, das im Chip verwendet wurde, aus der IMSI
- Das HLR setzt das "Hotlining Flag" zu dieser IMSI. Der erste Call geht dann zu einem SC (Security Center) (das SC könnte auch das HLR/AC selbst sein)

Der erste Call: Endpersonalisierung des Chip

- Da der Chip und das AC jetzt den gleichen secret Key Ki_1 kennen, bucht der Chip im Netz ein (Die PIN ist 0000 und dem Kunden bekannt)
- Der erste Call wird wegen Hotlining automatisch zum SC geroutet. Je nach Software im toolkit-fähigen Endgerät könnte der erste call bereits eine Short Message sein
- Das SC nutzt die Toolkitfähigkeit des Chip aus und handelt mit dem Chip einen neuen secret key Ki_2 aus.

Hierbei wird das Verfahren nach Diffie-Hellmann verwendet, das folgende Vorteile bietet:

- beliebig lange Keys sind aushandelbar
- Abhören auf der Luftschnittstelle reicht nicht aus, den generierten Schlüssel auszuspähen.

Der Chip speichert den neuen Key Ki_2 ab (dieser wird im folgenden zur Authentifikation verwendet).

- Der neue Key kann sofort verifiziert werden (z. B. challenge respone wie bei GSM üblich)
- Das SC überträgt den neuen Ki_2 an das AC
- Ebenfalls per Diffie-Hellman handelt das SC auch einen PUK (oder weitere Geheimzahlen) mit dem Chip aus. (Der Netzbetreiber kann dem Kunden die Geheimzahlen anschließend mitteilen oder auch für Service-Zwecke selbst behalten)
- Im HLR wird das Hotlining Flag entfernt. Damit sind jetzt reguläre Calls möglich, wobei ab diesem Zeitpunkt der neue secret Key Ki_2 verwendet wird
- Das toolkitfähige Endgerät informiert den Kunden über Erfolg oder Mißerfolg
- Das toolkitfähige Endgerät könnte dem Kunden anbieten, die PIN neu zu setzen

Wiederverwendung gebrauchter Chips/Karten

Sei das Teilnehmerverhältnis im HLR und AC ausgetragen, weil der Kunde gekündigt hat. Bei Vertragsabschluß mit dem neuen Kunden und dem gebrauchten Chip muß folgendes geschehen:
Zuerst wird die Funktion des Endgeräts zum Initialisieren des Chips genutzt. Daraufhin wird im Chip:

- Ki_2 wird gelöscht
- Ki_1 wird wieder aktiviert
- die PIN wird auf 0000 gesetzt
- der PUK wird auf 00000000 gesetzt (analog mit weiteren Geheimzahlen PUK2).

Diese Funktion könnte innerhalb des D1-Netzes beispielsweise der X13 aktivieren, der bei vielen Händlern steht. Damit hat der Händler wieder eine initiale Karte zum Vergeben.

Weiter geht es wie bei Kundengewinnung und Freischaltung durch den Netzbetreiber (s. o.)

Wechsel des secret key während der Nutzungsdauer des Chip

Der Netzbetreiber hat die Möglichkeit, in regelmäßigen Abständen einen Wechsel des Ki zu erzwingen. Dazu reicht es aus, im HLR das Hotlining-Flag zu setzen, den Call zum SC zu routen und wie oben beschrieben einen neuen Ki auszuhandeln. Der PUK sollte diesmal jedoch nicht neu ausgehandelt werden.

Mögliche Mißbrauchsszenarien (hier für D1 dargestellt)

1. Der Schlüssel K1 eines Chipherstellers ist kompromittiert und eine Karte wird nachgemacht
1.1 Die IMSI ist im AC noch nicht bekannt
Die Karte bucht nicht ein
1.2 Die IMSI der echten Karte ist bereits im AC und wurde bereits endpersonalisiert
Die falsche Karte bucht nicht ein, da Ki_1 ungleich Ki_2 ist (Authentifikation gescheitert)
1.3 Die echte IMSI ist bereits im AC, wurde aber noch nicht endpersonalisiert
Dies ist der kurze Zeitraum zwischen Vertragsabschluß und erstem Einschalten des Geräts. In dieser Zeit könnte sich eine Kartenfälschung "dazwischenschieben". Die echte Karte würde danach nicht einbuchen können, da sie nicht den Ki_2 der Fälschung besitzt. Dieses Szenario könnte organisatorisch vermieden werden, z. B. indem bei der Subscription eine Geheimzahl auf das Auftragsformular geschrieben wird, die der Kunde nach dem Schlüssel-Aushändigen eingeben muß, die zum SC geschickt wird und dort geprüft wird.
2. Der Kunde macht seine eigene Karte initial (z. B. mit X13)
Die Karte hat danach den Ki_1 und bucht nicht mehr ein.

Die Erfindung wird nun anhand eines Ausführungsbeispiels anhand der Zeichnungen näher beschrieben. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere Merkmale und Vorteile hervor.

Es zeigen:

Fig. 1: Schematisiert die Vorpersonalisierung der Karten beim Kartenhersteller;

Fig. 2: Schematisiert die Vorgänge beim Freischalten durch den Netzbetreiber (Endpersonalisierung);

Fig. 3: Schematisiert die Vorgänge beim Löschen des Chips und bei der Wiederverwendung.

In **Fig.** 1 ist zeichnerisch dargestellt, was bereits schon auf Seite 4 der Beschreibung angegeben ist, daß nämlich die Kartennummer ICCID in einem Bereich von einer Zahl X bis zu einer Zahl Y vorliegt.

Gleiches gilt für die Teilnehmerkennung IMSI, die ebenfalls in einem Zahlenbereich von A–B vorliegt.

Innerhalb der beiden Nummernbereiche für die ICCID und für die IMSI wird ferner eine Zahl a als Basis für die Diffie-Hellman gewählt und ebenso eine Zahl p, die als Primzahl für die Diffie-Hellman-Verschlüsselung dient.

Es wird ferner eine VER definiert, die als Funktionsnummer 8 Byte lang sein kann und ferner wird der Schlüssel K1 als DES-Schlüssel errechnet, der an VER gebunden ist.

Die genannten Daten werden in die Karte eingeschrieben und hierbei generiert (errechnet) der Chip dann die Geheimzahl Ki_1. welche in der Karte gespeichert wird. Die Karte wird in dieser Form (Vorpersonalisierung) an die VO (Verkaufsorganisation) ausgeliefert.

In **Fig.** 2 sind die einzelnen Vorgänge beschrieben, die ab Seite 5 der Beschreibung dargestellt sind.

Die VO geht in einem ersten Verfahrensschritt mit dem Kunden einen Vertrag ein. Im gleichen Verfahrensschritt wird die Kartennummer ICCID und die Versionsnummer in einer Auftragsbestätigung zusammen mit dem Vertrag eingetragen und diese Auftragsbestätigung wird in einem zweiten Verfahrensschritt zusammen mit der Teilnehmerkennung und der Versionsnummer VER an das AC mitgeteilt.

Gleichzeitig wird durch Mitteilung der Teilnehmerkennung IMSI an das HLR dafür gesorgt, daß das HLR die Kartendaten zur Kenntnis erhält und das sogenannte Hotlining Flag einrichtet.

Der Kunde erhält nun seine vorpersonalisierte Karte und nimmt mit dem ersten Anruf – der im Sinne der vorliegenden Erfindung zwangsläufig auf das SC geschaltet ist – Kontakt mit dem SC auf, wobei bei diesem ersten Anruf die Ki_2 ausgehandelt wird, ebenso wie die PUK und gleichzeitig wird auch die PIN neu gesetzt. Das SC andererseits verifiziert die geheime Schlüsselzahl Ki_2 gegenüber der Karte.

In einem vierten Verfahrensschritt nimmt SC Kontakt mit dem HLR auf und entfernt das Hotlining Flag, was dem Kunden nun die Möglichkeit gibt, beliebige Calls abzusetzen.

Das SC teilt im vierten Verfahrensschritt gleichzeitig die geheime Schlüsselzahl Ki_2 dem AC mit.

Damit ist die Karte freigeschaltet und endpersonalisiert.

Die Wiederverwendung gebrauchter Karten ist auf Seite der Beschreibung näher dargestellt. Hierbei ist in **Fig.** 3 erkennbar, daß der Kunde mit seiner Karte sich an die VO wendet, welche durch Eintragung der Kartennummer ICCID in die Auftragsbestätigung dafür sorgt, daß im AC die IMSI gelöscht wird und gleichzeitig auch im HLR.

Damit wird auch die Ki_2 gelöscht und die Ki_1 wird wieder aktiviert und in die Karte eingespeichert. Ebenso wird die PIN auf den Wert 0000 gesetzt und ebenfalls die PUK.

Die so wieder vorpersonalisierte Karte kann denn in einen Kartenpool eingestellt werden und für neue Kunden vergeben werden.

Die Endpersonalisierung wurde also wieder rückgängig gemacht und des liegt wieder der Zustand der Karte vor, wie er zum Zeitpunkt der Vorpersonalisierung bestand.

Es sei noch angemerkt, daß die Stelle des Netzbetreibers, bei welcher die Auftragsbestätigung abgewickelt wird, als Auftragsannahmestelle bezeichnet wird und diese Auftragsannahmestelle kennt die Zuordnungen von ICCID zu IMSI wegen der 1 : 1-Zuordnung innerhalb des vergebenen Nummernbereiches.

Patentansprüche

1. Verfahren zur Personalisierung von GSM-Chips, in deren Speicherbereich mindestens eine Teilnehmer-Kennung IMSI und eine Kartennummer ICCID eingespeichert sind, und wobei zwecks Personalisierung dem Chip noch ein geheimer Schlüssel Ki und weitere Daten eingespeichert sind, **dadurch gekennzeichnet**, daß die Personalisierung des Chips dann erfolgt, wenn der Teilnehmer sich in das Teilnehmernetz einbucht.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Personalisierung des Chips dann erfolgt, wenn der Teilnehmer sich erstmals in das Teilnehmernetz einbucht.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß zur Vorpersonalisierung des Chips beim Hersteller zunächst initiale, kartenbezogene Daten, nämlich ein erster, geheimer Schlüssel Ki_1 und weitere Daten, wie PIN und PUK eingespeichert werden.
4. Verfahren nach einem der Ansprüche 1–3, gekenn-

zeichnet durch folgende Verfahrensschritte:
in einem ersten Verfahrens schritt entnimmt der Chiphersteller die Kartennummer ICCID und die Teilnehmer-Kennung IMSI einem Nummernpool, der Chip selbst leitet sich aus einem Schlüssel K1, den der Chiphersteller kennt und in den Chip einbringt, den initialen, ersten Schlüssel Ki_1 ab, PIN und PUK werden auf einen Defaultwert gesetzt,
in einem zweiten Verfahrensschritt erfolgt ein Eintrag im AC und HLR, sobald ein Teilnehmer einen Vertrag mit dem Netzbetreiber geschlossen hat,
in einem dritten Verfahrensschritt leitet sich das AC ebenfalls den initialen, ersten Schlüssel Ki_1 ab,
in einem vierten Verfahrensschritt setzt das Netz die Bedingungen, damit beim Einbuchen ins Netz eine Verbindung vom Chip zur Komponente SC (Security Center des Netzbetreibers) entsteht,
in einem fünften Verfahrensschritt wird beim ersten Einbuchen die Verbindung vom Chip zum SC geschaltet,
in einem sechsten Verfahrensschritt wird im SC ein neuer, zweiter, geheimer Schlüssel Ki_2, sowie ein PUK mit dem Chip ausgehandelt (z. B. mit dem Verfahren nach Diffie-Hellman) oder im SC erzeugt und zum Chip übertragen,
in einem siebten Verfahrensschritt werden die Bedingungen aus Verfahrensschritt 4 wieder ausgeschaltet.

5. Verfahren nach einem der Ansprüche 1–4, dadurch gekennzeichnet, daß der erstmalig in den Chip eingespeicherte, initiale, geheime Schlüssel Ki_1 vor Vertragsabschluß nicht in das AC übertragen und dort gespeichert wird.

6. Chip zur Ausübung des Verfahrens nach einem der Ansprüche 1–5, dadurch gekennzeichnet, daß der Chip im Endgerät toolkitfähig ist, und mit dem SC kommunizieren kann und einen Schlüssel aushandeln kann.

7. Chip nach Anspruch 6, dadurch gekennzeichnet, daß der Chip Daten aus dem SC empfangen kann und diese in seinen Speicher einschreibt und Daten aus dem Speicher ausliest, verändert und/oder zum SC überträgt.

8. Chip nach einem der Ansprüche 6 oder 7, dadurch gekennzeichnet, daß sein Mikroprozessor einen geheimen Schlüssel mit dem SC aushandelt.

9. Chip nach Anspruch 8, dadurch gekennzeichnet, daß zum Aushandeln des Schlüssels das Verfahren nach Diffie-Hellman verwendet wird.

10. Chip nach einem der Ansprüche 6–9, dadurch gekennzeichnet, daß der Chip eine vom Hersteller fest programmierte Rufnummer enthält (fixed dialing).

11. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1–5, dadurch gekennzeichnet, daß das HLR geeignet ist, einen Umleitungsbefehl (Hotlining-Flag) zu setzen und zu löschen.

12. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1–5, unter Verwendung eines Chips nach einem der Ansprüche 6–10, dadurch gekennzeichnet, daß das Netz die Bedingungen setzt, damit beim Einbuchen ins Netz eine Verbindung vom Chip zur Komponente SC entsteht.

13. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1–5, unter Verwendung eines Chips nach einem der Ansprüche 6–10, dadurch gekennzeichnet, daß mit der erstmaligen Eintragung des initialen Schlüssel Ki_1 in das AC auch der Umleitungsbefehl (Hotlining-Flag) im HLR gesetzt wird.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

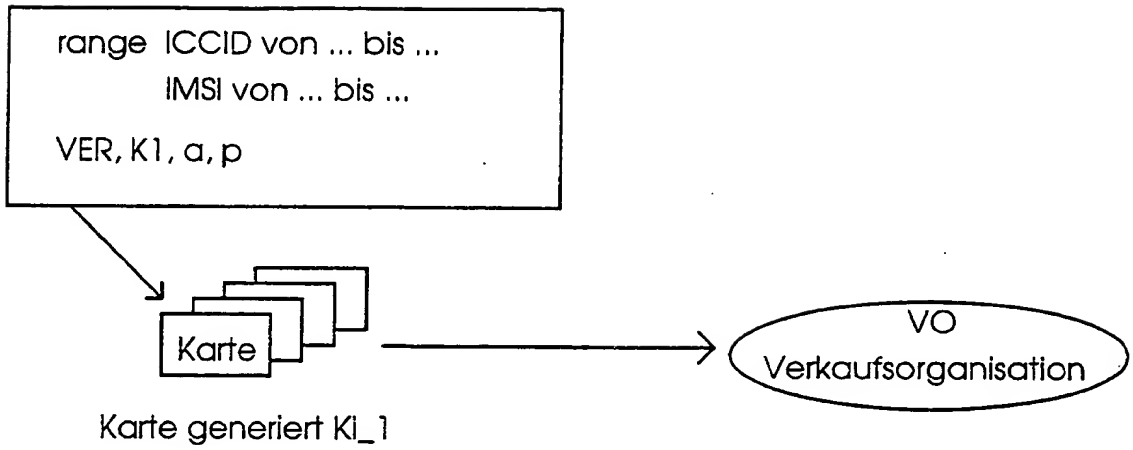
range ICCID von ... bis ...
IMSI von ... bis ...
VER, K1, a, p
Karte
VO
Verkaufsorganisation
Karte generiert Ki_1

Fig. 1

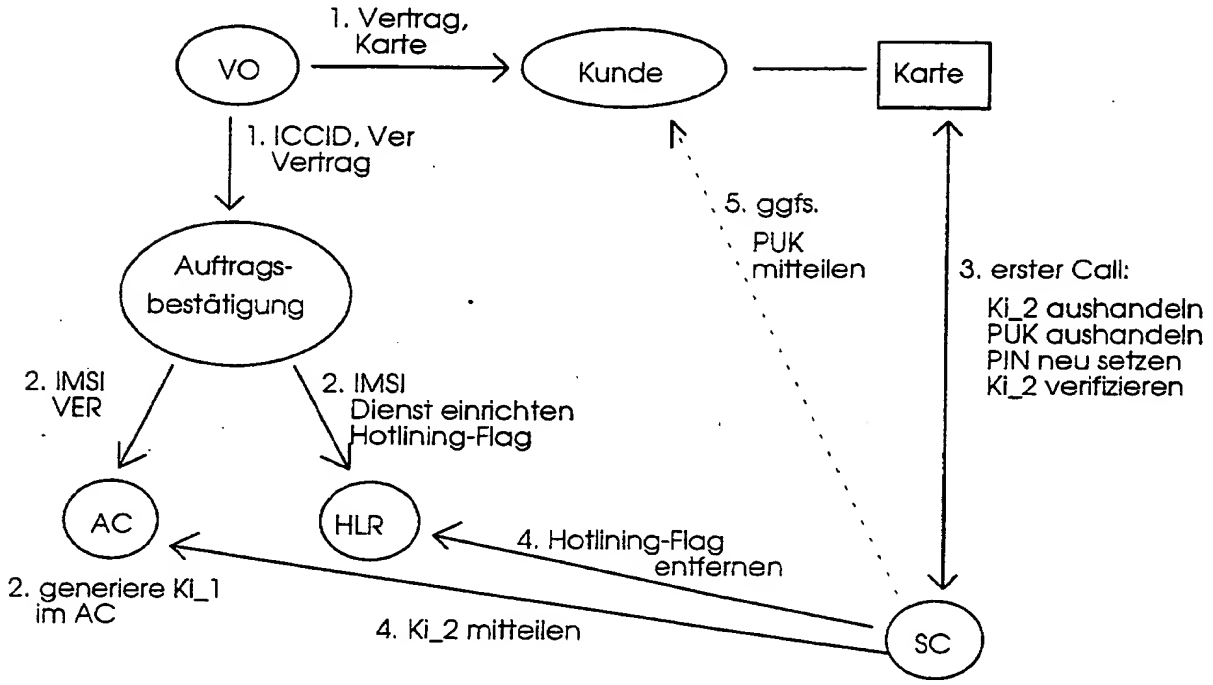
VO
1. Vertrag, Karte
Kunde
Karte
1. ICCID, Ver Vertrag
Auftrags-bestätigung
5. ggfs. PUK mitteilen
3. erster Call:
Ki_2 aushandeln
PUK aushandeln
PIN neu setzen
Ki_2 verifizieren
2. IMSI VER
2. IMSI Dienst einrichten Hotlining-Flag
AC
HLR
4. Hotlining-Flag entfernen
2. generiere Ki_1 im AC
4. Ki_2 mitteilen
SC

Fig. 2

Nummer: DE 197 33 662 C1
Int. Cl.: H 04 Q 7/34
Veröffentlichungstag: 7. Januar 1999

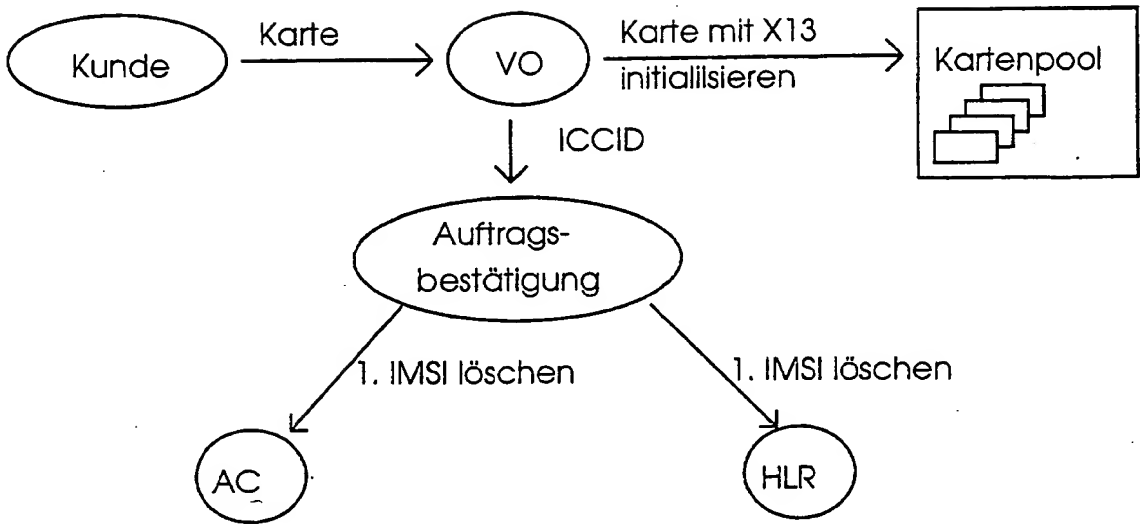

Fig. 3